REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1, 7, 11-13, 15, 18, 22-25, 27, and 28 are amended. Claims 17, 21, and 26 are canceled without prejudice. New claims 31-37 are added. Claims 1-16, 18-20, 22-25, and 27-37 are pending in this application.

Allowable Subject Matter

Claims 7, 8, 15, 16, and 25 stand objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form. As part of this Response, claims 7, 15, and 25 have been rewritten in independent form. Claim 8 depends from claim 7, and claim 16 depends from claim 15. Accordingly, Applicant respectfully submits that claims 7, 8, 15, 16, and 25 are in condition for allowance.

35 U.S.C. § 102

Claims 18, 19, 21, 22, and 26 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,108,644 to Goldschlag et al. (hereinafter "Goldschlag"). Claims 21 and 26 have been canceled without prejudice, thereby rendering the rejection of claims 21 and 26 moot. Applicant respectfully submits that claims 18, 19, and 22 are not anticipated by Goldschlag.

Goldschlag is directed to a system and method for electronic transactions (see, Title). A registrar receives an initialization request message that atomically binds authorization data with a blinded unvalidated certificate to be validated (see, col. 5, lines 44 – 47). The registrar determines if the authorization data is valid

(see, col. 5, line 56). If it is determined to be valid, then the blinded unvalidated certificate is validated to obtain a blinded validated certificate (see, col. 5, lines 57-59). The registrar party then sends an initialization response message that includes the blinded validated certificate atomically bound to the initialization request message (see, col. 5, lines 60-63). The initialization request message can be atomically bound to the initialization response message by including in both a secret encrypted session key that reliably identifies both messages as being bound to each other (see, col. 5, lines 63-67).

In contrast, amended claim 18 recites:

> An apparatus to digitally sign electronic information, the apparatus comprising:
>
> a connection module to establish a secure connection with a client device;
>
> a signature module to receive electronic information from the client device and digitally sign the electronic information, encoding attributes of the client device into the digital signature by basing the digital signature on at least a portion of a key in which the attributes are encoded.

Applicant respectfully submits that Goldschlag does not disclose or suggest a signature module to receive electronic information from the client device and digitally sign the electronic information, encoding attributes of the client device into the digital signature by basing the digital signature on at least a portion of a key in which the attributes are encoded as recited in amended claim 18.

Goldschlag includes no discussion of how a key is generated, much less having a key in which attributes of the client device are encoded as recited in amended claim 18. As there is no discussion of key generation in Goldschlag, Applicant respectfully submits that Goldschlag cannot disclose or suggest the signature module as recited in amended claim 18.

Thus, for at least these reasons, Applicant respectfully submits that amended claim 18 is allowable over Goldschlag.

Given that claim 19 depends from amended claim 18, Applicant respectfully submits that claim 19 is likewise allowable over Goldschlag for at least the reasons discussed above with respect to amended claim 18.

With respect to claim 22, claim 22 has been amended to depend from claim 23. Applicant respectfully submits that claim 22 is allowable over the cited references for at least the reasons discussed below with respect to claim 23.

Applicant respectfully requests that the §102 rejections be withdrawn.

35 U.S.C. § 103

Claims 1-6, 10-14, 17, 20, 23, 24, and 27-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Goldschlag in view of U.S. Patent No. 6,212,634 to Geer, Jr. et al. (hereinafter "Geer"). Claim 17 has been canceled without prejudice, thereby rendering the rejection of claim 17 moot. Applicant respectfully submits that claims 1-6, 10-14, 20, 23, 24, and 27-30 are not obvious over Goldschlag in view of Geer.

Geer is directed to a system for certifying authorizations that includes an authorizing computer and an authorized computer interconnected by a computer network. The authorizing computer creates a public key pair comprising a new public key and a new private key, and creates an authorization certificate that certifies that a holder of the authorization certificate is authorized to perform an action referred to in the authorization certificate. The authorization certificate includes the new public key. The authorizing computer causes the authorization

certificate and the new private key to be transmitted to the authorized computer. The authorized computer receives the authorization certificate and the new private key and decrypts messages using the new private key as evidence that the authorized computer has obtained the authorization certificate legitimately. See, Abstract.

With respect to amended claim 1, Applicant respectfully submits that Goldschlag in view of Geer does not disclose or suggest a certifying authority to digitally sign the blinded certificate and encode security attributes of the client device into at least a portion of a key on which the digital signature is based as recited in amended claim 1. As discussed above with respect to claim 18, Goldschlag makes no mention of how keys are generated. Thus, Applicant respectfully submits that Goldschlag does not disclose or suggest the certifying authority to encode security attributes of the client device into at least a portion of a key on which the digital signature is based as recited in amended claim 1.

With respect to Geer, Geer also includes no discussion of how keys are generated. Although Geer does discuss public key pairs, and also mentions that a public key pair can be created (see, for example, col. 3, lines 9-13 and 58-61). However, Geer does not discuss how such public key pairs are created. As there is no such discussion of how key pairs are created in Geer, Applicant respectfully submits that Geer cannot disclose or suggest a certifying authority to encode security attributes of the client device into at least a portion of a key on which the digital signature is based as recited in amended claim 1.

Thus, given that neither Goldschlag nor Geer discloses or suggests a certifying authority as recited in amended claim 1, Applicant respectfully submits

that Goldschlag in view of Geer does not disclose or suggest the certifying authority of amended claim 1. Thus, for at least these reasons, Applicant respectfully submits that amended claim 1 is allowable over Goldschlag in view of Geer.

Given that claims 2-6 depend from amended claim 1, Applicant respectfully submits that claims 2-6 are likewise allowable over Goldschlag in view of Geer for at least the reasons discussed above with respect to amended claim 1.

With respect to claim 9, claim 9 recites:

> A method comprising:
>
> receiving, from a client, a current certificate and a request to sign a new certificate;
>
> determining attributes of the client based on the current certificate;
>
> selecting, in accordance with public key cryptography, a public/private key pair that is based at least in part on the attributes of the client; and
>
> digitally signing the new certificate using the selected private key.

Applicant respectfully submits that Goldschlag in view of Geer does not disclose or suggest selecting, in accordance with public key cryptography, a public/private key pair that is based at least in part on the attributes of the client as recited in claim 9.

In the February 13, 2004 Office Action, it is acknowledged that Goldschlag makes no mention of selecting a public/private key pair that is based at least in part on the attributes of the client and also signing the new certificate with the selected private key (see, February 13 Office Action at p. 6, middle). In the February 13 Office Action, it is further asserted that "Geer teaches in column 1,

lines 8-10, that it is known to have certifying authorities that generate public key certificates that are enciphered with the private key of the certifying authority" (see, February 13 Office Action at p. 6, middle).

Applicant respectfully submits that the cited portion of Geer does not disclose or suggest the selecting of claim 9. The cited portion of Geer states that "Certifying authorities are known that generate public key certificates, enciphered with the private key of the certifying authority . . ." (see, Geer at col. 1, lines 8-10). However, Applicant respectfully submits that the mere mention of public key certificates and private keys does not disclose or suggest selecting a public/private key pair that is based at least in part on the attributes of the client. There is nothing in the cited portion of Geer, or elsewhere in Geer, that discusses how keys are generated in Geer. As there is no such discussion, Applicant respectfully submits that Geer cannot disclose or suggest selecting a public/private key pair that is based at least in part on the attributes of the client as recited in claim 9. Simply creating a new key pair does not disclose selecting a key pair based at least in part on the attributes of the client as recited in claim 9.

Thus, for at least these reasons, Applicant respectfully submits that neither Goldschlag nor Geer discloses or suggests the selecting of claim 9, and thus that claim 9 is allowable over Goldschlag in view of Geer.

Given that claims 10-12 depend from claim 9, Applicant respectfully submits that claims 10-12 are likewise allowable over Goldschlag in view of Geer for at least the reasons discussed above with respect to claim 9.

With respect to claim 13, claim 13 depends from claim 9, and Applicant respectfully submits that claim 13 is allowable over Goldschlag in view of Geer

for at least the reasons discussed above with respect to claim 9. Furthermore, Applicant respectfully submits Goldschlag in view of Geer does not disclose or suggest a method as recited in claim 9, wherein the selecting comprises determining a bit pattern that corresponds to the security attributes of the client, and identifying a public/private key pair that corresponds to the bit pattern as recited in claim 13.

As discussed above, there is no discussion in either Goldschlag or Geer of how keys are generated. As such, Applicant respectfully submits that there cannot be any discussion in either Goldschlag or Geer of determining a bit pattern that corresponds to security attributes of a client, and identifying a public/private key pair that corresponds to the bit pattern as recited in claim 13.

Thus, for at least these reasons, Applicant respectfully submits that claim 13 is allowable over Goldschlag in view of Geer.

With respect to claim 20, claim 20 depends from amended claim 18, and Applicant respectfully submits that claim 20 is allowable over Goldschlag for at least the reasons discussed above with respect to amended claim 18. Furthermore, similar to the discussions above, Applicant respectfully submits that Geer does not disclose or suggest encoding attributes of the client device into the digital signature by basing the digital signature on at least a portion of a key in which the attributes are encoded as recited in amended claim 18. Thus, Applicant respectfully submits that neither Goldschlag nor Geer discloses or suggests a signature module as recited in amended claim 18. Thus, for at least these reasons, Applicant respectfully submits that amended claim 18 and claim 20, which depends from amended claim 18, are allowable over Goldschlag in view of Geer.

With respect to claim 23, claim 23 has been rewritten to include the elements of its base claim, claim 21. Applicant respectfully submits that, similar to the discussions above, neither Goldschlag nor Geer discloses or suggests determining a public key based on a set of claimed security attributes, and using the public key to verify the digital signature as recited in claim 23. Thus, for at least these reasons, Applicant respectfully submits that claim 23 is allowable over Goldschlag in view of Geer.

Given that claims 22 and 24 depend from claim 23, Applicant respectfully submits that claims 22 and 24 are likewise allowable over Goldschlag in view of Geer for at least the reasons discussed above with respect to claim 23.

With respect to amended claim 27, amended claim 27 recites:

> A method comprising:
> generating a public/private key pair for use in public key cryptography;
> creating a certificate including the public key;
> transmitting the certificate to a certificate archive;
> receiving, from the certificate archive, an indication of whether the certificate is currently valid; and
> repeating the generating, creating, transmitting, and receiving for additional certificates until an indication that one of the certificates is currently valid is received.

Applicant respectfully submits that, similar to the discussion below regarding claim 29, Goldschlag in view of Geer does not disclose or suggest a method, including repeating the generating, creating, transmitting, and receiving for additional certificates until an indication that one of the certificates is currently valid is received as recited in amended claim 27. For at least these reasons, Applicant respectfully submits that amended claim 27 is allowable over Goldschlag in view of Geer.

Given that claim 28 depends from amended claim 27, Applicant respectfully submits that claim 28 is likewise allowable over Goldschlag in view of Geer for at least the reasons discussed above with respect to amended claim 27.

With respect to claim 29, Applicant respectfully submits that Goldschlag in view of Geer does not disclose or suggest a method for recovering from a device failure in a public key encryption system, the method comprising the acts (a) through (e), as recited in claim 29.

In the February 13 Office Action, it was asserted (at p. 11, middle) that:

> Geer teaches in column 1, lines 8-17, that it is known to have certifying authorities generate certificates based upon the public keys of the parties attempting to become certified or verified. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Geer's teachings on the use of public keys used in a certification/validation process into Goldschlag's design in order to achieve a design that is capable generating new certificate based public keys if it is determined that previous certificates were not valid.

The cited portion of Geer, column 1 at lines 8-17 (see, February 13 Office Action at p. 10, bottom) is as follows:

> Certifying authorities are known that generate public key certificates, enciphered with the private key of the certifying authority, that serve as letters of introduction of a particular party to any other party that can recognize the certifying authority as an introducer. The certifying authority typically makes the party seeking the certificate of introduction prove that it is who it says it is, and then the certifying authority accepts the public key of the party and returns it in the certificate of introduction signed with the private key of the certifying authority, thereby binding the name of the particular party to the public key of the party.

As can be seen from this discussion in Geer, the certifying authority typically makes the party seeking the certificate of introduction prove that it is

who it says it is, and then returns the public key of the party in a certificate of introduction signed with the private key of the certifying authority. There is no indication or discussion in Geer that the certifying authority performs any sort of repeated certificate generation to determine whether a certificate is currently valid. Thus, Applicant respectfully submits that Geer does not disclose or suggest repeating acts (b) through (d) of claim 29 until a valid certificate is created as recited in claim 29. The mere mention of public key certificates and key pairs being created does not disclose or suggest repeating the creating, querying, and generating as recited in acts (b) through (e) of claim 29 until a valid certificate is created as recited in claim 29.

Furthermore, there is no discussion or suggestion in Geer or Goldschlag that simply creating a new certificate and querying whether that new certificate is valid would result in a valid certificate. Nowhere in Geer or Goldschlag is there any discussion of why creating a new certificate would be desirable, much less of how to create a new certificate that would be valid when a previous certificate was not valid. Thus, Applicant respectfully submits that there cannot be any disclosure or suggestion in Geer or Goldschlag of the repeating of acts (b) through (d) until a valid certificate is created as recited in claim 29.

Thus, for at least these reasons, Applicant respectfully submits that claim 29 is allowable over Goldschlag in view of Geer.

Given that claim 30 depends from claim 29, Applicant respectfully submits that claim 30 is likewise allowable over Goldschlag in view of Geer for at least the reasons discussed above with respect to claim 29.

Claims 6 and 14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Goldschlag and Geer in view of U.S. Patent No. 4,759,063 to Chaum (hereinafter "Chaum"). Applicant respectfully submits that claims 6 and 14 are not obvious over Goldschlag and Geer in view of Chaum.

With respect to claim 6, Applicant respectfully submits that Chaum is not cited as curing, and does not cure, the deficiencies of Goldschlag and Geer as discussed above with respect to amended claim 1. Thus, for at least these reasons, Applicant respectfully submits that claim 6 is allowable over Goldschlag and Geer in view of Chaum.

With respect to claim 14, Applicant respectfully submits that Chaum is not cited as curing, and does not cure, the deficiencies of Goldschlag and Geer as discussed above with respect to claim 9. Thus, for at least these reasons, Applicant respectfully submits that claim 14 is allowable over Goldschlag and Geer in view of Chaum.

Applicant respectfully requests that the §103 rejections be withdrawn.

New Claims

New claims 31-37 are added.

With respect to new claim 31, Applicant respectfully submits that the cited references do not disclose or suggest one or more computer-readable media containing a plurality of instructions that, when executed by one or more processors, causes the one or more processors to: receive, from a client, a current certificate and a request to sign a new certificate; determine attributes of the client based on the current certificate; select, in accordance with public key

cryptography, a public/private key pair that is based at least in part on the attributes of the client; and digitally sign the new certificate using the selected private key as recited in new claim 31. For at least these reasons, Applicant respectfully submits that new claim 31 is allowable over the cited references.

With respect to new claim 32, new claim 32 depends from claim 31, and Applicant respectfully submits that new claim 32 is allowable over the cited for at least the reasons discussed above with respect to claim 31. Furthermore, Applicant respectfully submits that the cited references do not disclose or suggest one or more computer-readable media as recited in claim 31, wherein the attributes are security attributes of the client as recited in new claim 32. For at least these reasons, Applicant respectfully submits that new claim 32 is allowable over the cited references.

With respect to new claim 33, new claim 33 depends from claim 31, and Applicant respectfully submits that new claim 33 is allowable over the cited for at least the reasons discussed above with respect to claim 31. Furthermore, Applicant respectfully submits that the cited references do not disclose or suggest one or more computer-readable media as recited in claim 31, wherein the new certificate is a blinded certificate as recited in new claim 33. For at least these reasons, Applicant respectfully submits that new claim 33 is allowable over the cited references.

With respect to new claim 34, new claim 34 depends from claim 31, and Applicant respectfully submits that new claim 34 is allowable over the cited for at least the reasons discussed above with respect to claim 31. Furthermore, Applicant respectfully submits that the cited references do not disclose or suggest

one or more computer-readable media as recited in claim 31, wherein the instructions that cause the one or more processors to select the public/private key pair further cause the one or more processors to determine a bit pattern that corresponds to the security attributes of the client, and identify a public/private key pair that corresponds to the bit pattern as recited in new claim 34. For at least these reasons, Applicant respectfully submits that new claim 34 is allowable over the cited references.

With respect to new claim 35, Applicant respectfully submits that the cited references do not disclose or suggest one or more computer-readable media containing a plurality of instructions that, when executed by one or more processors, causes the one or more processors to: receive, from a client, a request for electronic content; check, based on information encoded in a digital signature of at least a portion of the request, whether the client has a set of claimed security attributes by determining a public key based on the set of claimed security attributes and using the public key to verify the digital signature; and determine how to respond to the request based on the checking as recited in new claim 35. For at least these reasons, Applicant respectfully submits that new claim 35 is allowable over the cited references.

With respect to new claim 36, new claim 36 depends from claim 35, and Applicant respectfully submits that new claim 36 is allowable over the cited for at least the reasons discussed above with respect to claim 35. Furthermore, Applicant respectfully submits that the cited references do not disclose or suggest one or more computer-readable media as recited in claim 35, wherein the instructions that cause the one or more processors to check whether the client has a

set of claimed security attributes further cause the one or more processors to represent the set of claimed security attributes as a series of bits and generate the public key using the series of bits as recited in new claim 36. For at least these reasons, Applicant respectfully submits that new claim 36 is allowable over the cited references.

With respect to new claim 37, new claim 37 depends from claim 36, and Applicant respectfully submits that new claim 37 is allowable over the cited for at least the reasons discussed above with respect to claim 36. Furthermore, Applicant respectfully submits that the cited references do not disclose or suggest one or more computer-readable media as recited in claim 36, wherein the instructions that cause the one or more processors to generate the public key further cause the one or more processors to: identify, for each bit in the series that has a particular value, a corresponding integer; and generate as the public key the product of the identified integers as recited in new claim 37. For at least these reasons, Applicant respectfully submits that new claim 37 is allowable over the cited references.

Conclusion

Claims 1-16, 18-20, 22-25, and 27-37 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 5/13/04

By: _____

Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256